UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSEPH COE, individually and on behalf of all others similarly situated, Plaintiff, v. NORTHEAST ORTHOPEDICS AND SPORTS MEDICINE, PLLC, Defendant.	Case No. 24-cv-1975 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Joseph Coe, individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Northeast Orthopedics and Sports Medicine, PLLC ("Northeast Orthopedics" or "Defendant"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Northeast Orthopedics for its failure to secure and safeguard his and approximately 177,276 other individuals' personally identifying information ("PII") and personal health information ("PHI"), including names, Social Security numbers, driver's license information, payment information, dates of birth, medical record information, health insurance information, and treatment and diagnosis information.

2. Northeast Orthopedics is a provider of orthopedic and musculoskeletal healthcare services.

3. On or about November 22, 2023, an unauthorized third party gained access to Northeast Orthopedics' network system and obtained files containing information about Northeast Orthopedics' current and former patients (the "Data Breach").

4. Northeast Orthopedics owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Northeast Orthopedics breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Northeast Orthopedics' inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach, which occurred on or about November 22, 2023.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of implied contract, unjust enrichment, and violations of New York General Business Law § 349, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Joseph Coe

7. Plaintiff Coe is a citizen of New York.

8. Plaintiff Coe obtained healthcare or related services from Northeast Orthopedics. As a condition of receiving services, Northeast Orthopedics required Plaintiff Coe to provide it with his PII/PHI.

9. Based on representations made by Northeast Orthopedics, Plaintiff Coe believed Northeast Orthopedics had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff Coe provided his PII/PHI to Northeast Orthopedics in connection with receiving healthcare or related services provided by Northeast Orthopedics.

10. At all relevant times, Northeast Orthopedics stored and maintained Plaintiff Coe's PII/PHI on their network systems.

11. Plaintiff Coe takes great care to protect his PII/PHI. Had Plaintiff Coe known that Northeast Orthopedics does not adequately protect the PII/PHI in its possession, he would not have obtained healthcare services from Northeast Orthopedics or agreed to entrust them with his PII/PHI.

12. Plaintiff Coe received a letter from Northeast Orthopedics notifying him that his PII/PHI was affected in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff Coe has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

Defendant Northeast Orthopedics and Sports Medicine, PLLC

14. Defendant Northeast Orthopedics and Sports Medicine, PLLC is a New York limited liability company with its headquarters located at 507 Airport Executive Park, Nanuet, New York 10954.

JURISDICTION AND VENUE

15. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. This Court has personal jurisdiction over Northeast Orthopedics because it is a New York corporation with its principal place of business in this District.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(2) because Northeast Orthopedics' principal place of business is located in this District, and a substantial part of the events giving rise to Plaintiff's claims arose in this District.

FACTUAL ALLEGATIONS

Overview of Northeast Orthopedics

18. Northeast Orthopedics provides "advanced musculoskeletal and related care," including general orthopedics, sports medicine, orthopedic surgery, diagnostic testing, and rheumatology services.[1] It has nine locations in southern New York.[2]

[1] *About Us*, NORTHEAST ORTHPEDICS & SPORTS MED., https://neosmteam.com/about-us/ (last accessed Mar. 15, 2024).
[2] *See Locations*, NORTHEAST ORTHPEDICS & SPORTS MED., https://neosmteam.com/locations/ (last accessed Mar. 15, 2024).

19. In the regular course of its business, Northeast Orthopedics collects and maintains the PII/PHI of its current and former patients. Northeast Orthopedics required Plaintiff and Class members to provide their PII/PHI as a condition of receiving healthcare services from Northeast Orthopedics.

20. Northeast Orthopedics' website contains a Notice of Privacy Practices (the "Privacy Policy").[3] The Privacy Policy "describe the ways that [Northeast Orthopedics] may use and disclose health information about [its] patients."[4] This includes for treatment, payment, and healthcare operations purposes.[5]

21. In the Privacy Policy, Northeast Orthopedics acknowledges it is required by HIPAA to "protect the privacy of health information that identifies a patient, or where there is a reasonable basis to believe the information can be used to identify a patient."[6] Northeast Orthopedics admits it is "required by law to . . . [m]aintain the privacy of PHI about you" and to comply with the terms of the Privacy Policy.[7]

22. Northeast Orthopedics promises "[o]ther uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described" in the Privacy Policy.[8]

---

[3] *Notice of Privacy Practices*, NORTHEAST ORTHPEDICS & SPORTS MED. (Apr. 14, 2003), https://neosmteam.com/wp-content/uploads/2018/08/16-09-06_PrivacyPolicy.pdf [hereinafter, the "*Privacy Policy*"].
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] *Id.*

The Data Breach

23. On or about November 22, 2023, an unknown actor accessed Northeast Orthopedics' systems and accessed certain files containing the PII/PHI of Plaintiff and Class members.[9] Through an investigation into the Data Breach, Northeast Orthopedics discovered that the type information affected by the Data Breach included "name, Social Security number, driver's license information, payment information, date of birth, medical record information, health insurance information, and treatment and diagnosis information."[10]

24. Though the Data Breach occurred on or about November 22, 2023, Northeast Orthopedics waited until February 2024, over two months later, to begin notifying its patients that their PII/PHI was in the hands of cybercriminals.[11]

25. Northeast Orthopedics' failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Defendant Knew that Criminals Target PII/PHI

26. At all relevant times, Northeast Orthopedics knew, or should have known, that the PII/PHI that it collected and stored was a target for malicious actors. Despite such knowledge, Northeast Orthopedics failed to implement and maintain reasonable and appropriate data privacy

---

[9] *Notice of Data Security Incident*, NORTHEAST ORTHPEDICS & SPORTS MED., https://neosmteam.com/notice-of-data-security-incident/ (last accessed Mar. 15, 2024).
[10] *Id*.
[11] *See id.*

and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks that it should have anticipated and guarded against.

27. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers ("SSNs") and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[12]

28. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found that there were 956 medical data breaches in 2022 with over 59 million patient records exposed.[13] This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.[14]

29. PII/PHI is a valuable property right.[15] The value of PII/PHI as a commodity is measurable.[16] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory

---

[12] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[13] *See* PROTENUS, *2023 Breach Barometer*, PROTENUS.COM, https://www.protenus.com/breach-barometer-report (last accessed Mar. 15, 2024).
[14] *See id*.
[15] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. PROCESSING 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[16] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), http://www.medscape.com/viewarticle/824192.

frameworks."[17] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[18] It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

30. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

31. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[19] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[20]

32. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each

[17] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.
[18] *See* IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.
[19] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon ("*What Happens to Stolen Healthcare Data*") (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[20] *Id.*

on the black market.[21] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[22]

33. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[23] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[24]

34. Consumers place a high value on the privacy of their PII/PHI. Consumers place considerable value in their data privacy. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[25]

35. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[21] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.

[22] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.

[23] Steager, *supra* note 19.

[24] *Id.*

[25] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

36. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[26] [27]

37. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[28]

38. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[29]

39. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate

---

[26] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Mar. 15, 2024).

[27] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[28] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[29] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Mar. 15, 2024).

ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

40. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[30]

41. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[31] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[32] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [33] The FTC also warns, "If the thief's health information is mixed with yours it

[30] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.
[31] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[32] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 22.
[33] *See What to Know About Medical Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed Mar. 15, 2024).

could affect the medical care you're able to get or the health insurance benefits you're able to use."[34]

42. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- Difficulty qualifying for a mortgage or other loans and other financial impact, as a result of improper and/or fraudulent medical debt reporting.
- Phantom medical debt collection based on medical billing or other identity information.
- The exacerbation of existing debt collection and credit problems due to the sales of medical debt arising from identity theft, through no fault of their own.[35]

43. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

[34] *Id*.
[35] *See* Dixon & Emerson, *supra* note 31.

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[36]

44. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiff and Class Members

45. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

46. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

47. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

All United States residents whose PII/PHI was accessed by unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

48. Excluded from the Class are Northeast Orthopedics and Sports Medicine, PLLC and its affiliates, parents, subsidiaries, employees, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

49. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

50. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. Northeast Orthopedics has reported to the Department of Health and Human Services that 177,101 persons were affected by the Data Breach.[37]

51. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. whether Defendant had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d. whether an implied contract existed between Class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class members' PII/PHI from unauthorized access and disclosure;

[37] *Cases Currently Under Investigation*, DEP'T HEALTH & HUM. SERVS., https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Mar. 15, 2024).

e. whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Plaintiff and Class members;

f. whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI; and

g. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

52. Northeast Orthopedics engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

53. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Northeast Orthopedics, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

54. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

55. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required

to individually litigate their claims against Northeast Orthopedics, so it would be impracticable for Class members to individually seek redress from Northeast Orthopedics' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

56. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

57. Northeast Orthopedics owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

58. Northeast Orthopedics knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Northeast Orthopedics knew or should have known of the many data breaches that targeted healthcare provides that collect and store PII/PHI in recent years.

59. Given the nature of Northeast Orthopedics' business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, Northeast Orthopedics should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

60. Northeast Orthopedics breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

61. It was reasonably foreseeable to Northeast Orthopedics that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

62. But for Northeast Orthopedics' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

63. As a result of Northeast Orthopedics' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Northeast Orthopedics' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

64. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

65. Northeast Orthopedics' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

66. Northeast Orthopedics duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Northeast Orthopedics, of failing to employ reasonable measures to protect and secure PII/PHI.

67. Northeast Orthopedics violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI, by failing to provide timely notice, and by not complying with applicable industry standards. Northeast Orthopedics' conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

68. Northeast Orthopedics' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

69. Plaintiff and Class members are within the class of persons that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

70. The harm occurring as a result of the Data Breach is the type of harm that the HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

71. It was reasonably foreseeable to Northeast Orthopedics that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

72. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Northeast Orthopedics' violations of the HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Northeast Orthopedics' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the

Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

73. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

74. Plaintiff and Class members gave Northeast Orthopedics their PII/PHI in confidence, believing that Northeast Orthopedics would protect that information. Plaintiff and Class members would not have provided Northeast Orthopedics with this information had they known it would not be adequately protected. Northeast Orthopedics' acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between Northeast Orthopedics and Plaintiff and Class members. In light of this relationship, Northeast Orthopedics must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

75. Due to the nature of the relationship between Northeast Orthopedics and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon Northeast Orthopedics to ensure that their PII/PHI was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of Northeast Orthopedics' data security policies and practices, and Northeast Orthopedics was in an exclusive position to guard against the Data Breach.

76. Northeast Orthopedics has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class

members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

77. As a direct and proximate result of Northeast Orthopedics' breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Northeast Orthopedics' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF IMPLIED CONTRACT

78. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

79. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Northeast Orthopedics.

80. Pursuant to these implied contracts, Plaintiff and Class members paid money to Northeast Orthopedics, directly or through their insurance, and provided Northeast Orthopedics with their PII/PHI. In exchange, Northeast Orthopedics agreed to, among other things, and Plaintiff and Class members understood that Northeast Orthopedics would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class

members' PII/PHI in compliance with federal and state laws and regulations and industry standards.

81. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Northeast Orthopedics, on the other hand. Indeed, as set forth *supra*, Northeast Orthopedics recognized the importance of data security and the privacy of its patients' PII/PHI. Had Plaintiff and Class members known that Northeast Orthopedics would not adequately protect their PII/PHI, they would not have received healthcare or other services from Northeast Orthopedics.

82. Plaintiff and Class members performed their obligations under the implied contract when they provided Northeast Orthopedics with their PII/PHI and paid for healthcare or other services from Northeast Orthopedics.

83. Northeast Orthopedics breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

84. Northeast Orthopedics' breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

85. Plaintiff and all other Class members were damaged by Northeast Orthopedics' breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to

unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT V
UNJUST ENRICHMENT

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. This claim is pleaded in the alternative to the breach of implied contract claim.

88. Plaintiff and Class members conferred a monetary benefit upon Northeast Orthopedics in the form of monies paid to Northeast Orthopedics for healthcare services and through the provision of their PII/PHI.

89. Northeast Orthopedics accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Northeast Orthopedics benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to provide healthcare services and facilitate billing services.

90. As a result of Northeast Orthopedics' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures, that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures, that they received.

91. Northeast Orthopedics should not be permitted to retain the money belonging to Plaintiff and Class members because Northeast Orthopedics failed to adequately implement the

data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

92. Plaintiff and Class members have no adequate remedy at law.

93. Northeast Orthopedics should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VI
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law § 349

94. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

95. New York General Business Law § 349(a) states, "Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

96. Northeast Orthopedics engaged in "business," "trade," or "commerce" within the meaning of § 349(a).

97. Plaintiff and Class members are "persons" within the meaning of Gen. Bus. Law § 349(h).

98. In its Privacy Policy, Northeast Orthopedics makes explicit statements to its patients regarding how their PII/PHI will be used and protected.

99. Northeast Orthopedics' failure to make Plaintiff and Class members aware that it would not adequately safeguard their information, while maintaining that it would, is a "deceptive act or practice" under Gen. Bus. Law § 349.

100. Had Plaintiff and Class members been aware that Northeast Orthopedics omitted or misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and

Class members would not have accepted healthcare or related services from Northeast Orthopedics.

101. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, Northeast Orthopedics' failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class now face a substantially higher risk of identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Northeast Orthopedics' practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

102. As a result of Northeast Orthopedics' violations of the Gen. Bus. Law § 349, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Northeast Orthopedics' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

103. Pursuant to Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of himself and the Class in the amount of the greater of actual damages or $50 for each violation of Gen. Bus. Law § 349. Because Northeast Orthopedics' conduct was committed willfully and knowingly, Plaintiff and Class members are entitled to recover up to three times their actual damages up to $1,000.

REQUEST FOR RELIEF

Plaintiff, individually and on behalf of all other Class members, respectfully requests that the Court enter judgment in his favor and against Northeast Orthopedics as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Northeast Orthopedics from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: March 15, 2024

Respectfully submitted,

/s/ *Adam Pollock*
Adam Pollock
Anna Menkova

POLLOCK COHEN LLP
111 Broadway, Suite 1804
New York, NY 10006
Tel: 212-337-5361
adam@pollockcohen.com
anna@pollockcohen.com

Ben Barnow
Anthony L. Parkhill*
Barnow and Associates, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Counsel for Plaintiff Joseph Coe

**pro hac vice forthcoming*